

---

PAT-NO: JP410293727A  
DOCUMENT-IDENTIFIER: JP 10293727 A  
TITLE: IN-MEMORY DATA SECURITY PROTECTION SYSTEM FOR  
IC CARD  
PUBN-DATE: November 4, 1998

---

INVENTOR-INFORMATION:

NAME  
TSUGANE, SHOICHI

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI LTD	N/A

APPL-NO: JP09104208

APPL-DATE: April 22, 1997

INT-CL (IPC): G06F012/14, G06K019/073

ABSTRACT:

PROBLEM TO BE SOLVED: To prevent the secret of in-memory data from being illegally read by damaging or decomposing secret data that is held in memory of an IC card, i.e., the IC card, forecedly sucking internal data up with a ROM writer, etc., analyzing the internal data and decoding cipher of key value, etc.

SOLUTION: When an IC card body 1 is damaged or disassembled, a bus that connects a battery 30 and memory 10 which are in a disconnection state with a switch correspondence function that works with the opening of the body 1 is brought into contact, the bus is connected, or external light strikes and the resistivity of a device 70 which is connected to the bus that

~~connects the~~

battery 30 and the memory 10 is increased. With this, voltage is applied to an external terminal for erasing data of the memory, all or a part of data held in the memory 10 is erased and the privacy of in-memory data is protected.

COPYRIGHT: (C)1998,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-293727

(43) 公開日 平成10年(1998)11月4日

(51) Int.Cl.<sup>4</sup>

識別記号

F I

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 D

G 0 6 K 19/073

G 0 6 K 19/00

P

審査請求 未請求 請求項の数2 O L (全 3 頁)

(21) 出願番号

特願平9-104208

(22) 出願日

平成9年(1997)4月22日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 津金 象一

神奈川県秦野市堀山下1番地 株式会社日

立製作所汎用コンピュータ事業部内

(74) 代理人 弁理士 小川 勝男

(54) 【発明の名称】 ICカードにおけるメモリ内データ機密保護方式

(57) 【要約】

【課題】本発明は、ICカード内のメモリに保持されている機密データを、ICカードを破壊あるいは分解し、ROMライター等により強制的に内部データを吸い上げ、内部データを解析し、キー値等の暗号を解読することにより、メモリ内データの機密を不当に読み込むことを防ぐことにある。

【解決手段】ICカード本体を破壊あるいは分解した場合、ICカード本体の開封と連動したスイッチ相当機能によって断線状態にあった電池とメモリを接続するバスが接触し、バスが結線することにより、あるいは、外部からの光が当たり、電池とメモリを接続するバスに接続されたデバイスの抵抗率が高くなることにより、メモリのデータ消去用外部端子に電圧が加わりメモリ内で保持しているデータの全てあるいは一部を消去し、メモリ内データの機密を保護する。

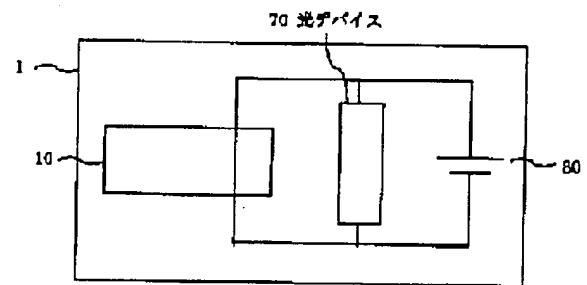


図4

## 【特許請求の範囲】

【請求項1】一定電圧がかかると保持しているデータを消去する外部端子を持つメモリと、電池と、ICカード本体の開封と連動したスイッチ相当機能によって断線状態になっている電池とメモリを接続するバスから成るICカードにおいて、ICカードを破壊あるいは分解した場合に、ICカード本体によって断線状態にあった電池とメモリを接続するバスが接触し、バスが結線することにより、電池による電圧がデータ消去用外部端子に加わり、保持しているデータの全てあるいは一部を消去し、メモリ内データの機密を保護するICカードにおけるメモリ内データ機密保護方式。

【請求項2】一定電圧がかかると保持しているデータを消去する外部端子を持つメモリと、電池と、光量によって抵抗率が高くなるデバイスと、メモリと電池を接続するバスから成るICカードにおいて、ICカードを破壊あるいは分解した場合に、光量によって抵抗率が高くなるデバイスに、外部からの光が当たり、電池による電圧がデータ消去用外部端子に加わり、保持しているデータの全てあるいは一部を消去することにより、メモリ内データの機密を保護するICカードにおけるメモリ内データ機密保護方式。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、ICカードにおけるメモリ内データを消去することにより機密を保護する、メモリ内データ機密保護方式に関する。

## 【0002】

【従来の技術】従来、ICカード内で保持しているメモリ内データの不当読み込みを防止する方法としては、特願平3-178550号公報に記載のように、内部に記憶回路を内蔵し、外部から読み出し可能なICカードにおいて、ICカード内のメモリのアドレス空間をいくつかのセグメントに分割し、それぞれのセグメントに対して1つのキー情報をカード内部に持ち、そのキー情報と外部より与えられたキー情報とを比較するためのコンパレータを持ち、各セグメントに対応したキー情報が全て正しい時のみICカードの読み出し結果を有効にする方式が提案されている。

## 【0003】

【発明が解決しようとする課題】上記した従来のメモリ内データ不当読み込み防御方式では、データをICカードから読み取る際に、暗号化を行い内部データの機密を保護しているが、ICカード内のメモリには機密データが保持されており、ICカードを破壊あるいは分解し、ROMライタ等により強制的に内部データを吸い上げ、内部データを解析し、キー値等の暗号を解説することにより、メモリ内データの機密を不当に読み込むことが出来る。

## 【0004】

【課題を解決するための手段】本発明によれば、ROMライタ等で直接ICカード内のメモリ・データにアクセスするために、ICカード本体を破壊あるいは分解した場合、ICカード本体の開封と連動したスイッチ相当機能によって断線状態にあった電池とメモリを接続するバスが接触し、バスが結線することにより、あるいは、外部からの光が当たり、電池とメモリを接続するバスに接続された光デバイスの抵抗率が高くなることにより、メモリのデータ消去用外部端子に電圧が加わりメモリ内で保持しているデータの全てあるいは一部を消去することにより、メモリ内データの機密を保護することが出来る。

## 【0005】

【発明の実施の形態】以下、本発明の好ましい実施例を説明する。

【0006】図1は、ICカードの回路図の内、請求項1の発明に関する部分を表している。スイッチ20が押下されると、接点21と接点22がスイッチ20を介して接続され、メモリ10は電池30と接続される。

【0007】図2は、ICカードの本体が密封されている場合のスイッチ部の状態を示している。

【0008】ICカードの本体が密封されている場合、スイッチ20は、本体1につながっているストッパ50の為に、接点21と接点22に接することが出来ない。この為、メモリ10は電池30と接続されず、データ消去用外部端子11に電圧が加わらない為、メモリ内データは保持されている。

【0009】図3は、ICカードを破壊あるいは分解した場合のスイッチ部の状態を示している。

【0010】ICカードを破壊あるいは分解した場合、スプリング60の反発力の為、ストッパ50は押下され、接点21と接点22がスイッチ20を介して接続され、メモリ10は電池30と接続される。この為、データ消去用外部端子11に電池30からの電圧が加わりメモリ内データは消去される。

【0011】図4は、ICカードの回路図の内、請求項2の発明に関する部分を表している。メモリ10は、光量に比例して抵抗率が高くなる光デバイス70と並列に電池30と接続されている。

【0012】ICカードの本体1が密封されている場合、外部の光は光デバイス70に当たらない為、光デバイス70の抵抗値は低くなっている。この為、光デバイス70に並列接続されているメモリ10のデータ消去用外部端子11には、メモリ内データを消去する為のしきい値よりも小さい電圧しか加わらない為、メモリ内データは保持されている。

【0013】ICカードを破壊あるいは分解した場合、外部の光が光デバイス70に当たり、光デバイス70の抵抗値は大きくなる。この為、メモリ10のデータ消去用外部端子11に、メモリ内データを消去する為のしき

3

い値よりも大きな電圧が加わり、メモリ内データは消去される。

【0014】以上の様に、請求項1及び請求項2における発明では、不当に第三者がICカードのメモリ内データを読み取ろうとしてICカードを破壊あるいは分解した場合、メモリ内データを消去することにより、メモリ内データの機密を保護することができる。

【0015】

【発明の効果】本発明によれば、ICカード本体を破壊あるいは分解した場合、ICカード本体によって断線状態にあった電池とメモリを接続するバスが接触し、バスが結線することにより、あるいは、外部からの光が当たり、電池とメモリを接続するバスに接続されたデバイスの抵抗率が高くなることにより、メモリのデータ消去用

4

外部端子に電圧が加わりメモリ内で保持しているデータの全てあるいは一部を消去し、メモリ内データの機密を保護することができる。

【図面の簡単な説明】

【図1】本発明請求項1による一実施例（回路図）。

【図2】正常時のスイッチ部の断面図。

【図3】ICカードを破壊あるいは分解した場合のスイッチ部の断面図。

【図4】本発明請求項2による一実施例（回路図）。

【符号の説明】

1…ICカード本体、10…メモリ、11…データ消去用端子、20…スイッチ、21…接点、22…接点、30…電池、40…基盤、50…ストッパ、60…スプリング、70…光デバイス。

【図1】

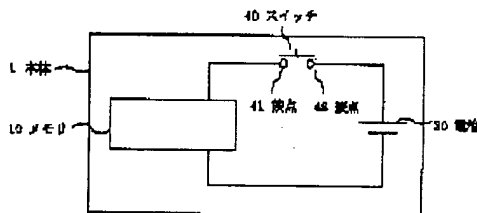


図1

【図2】

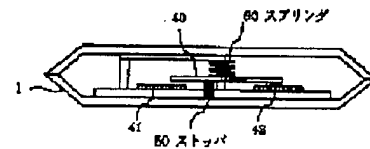


図2

【図3】

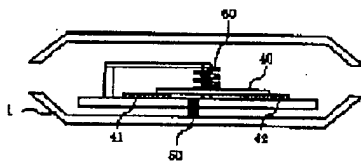


図3

【図4】

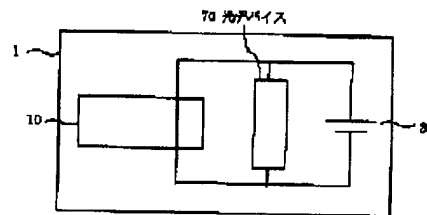


図4

---

\*NOTICES\*

---

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
  2. \*\*\*\* shows the word which can not be translated.
  3. In the drawings, any words are not translated.
- 

---

## DETAILED DESCRIPTION

---

### [Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the data security method in memory which protects secrecy by eliminating the data in memory in an IC card.

[0002]

[Description of the Prior Art] As an approach of preventing unjust reading of the data in memory currently held within an IC card, conventionally Like a publication in a Japanese-Patent-Application-No. No. 178550 [ three to ] official report, build a store circuit in the interior and it sets from the exterior to the IC card which can be read. The address space of the memory in an IC card is divided into some segments. It has one key information in the interior of a card to each segment. it has a comparator for comparing the key information with the key information given from the exterior, and the method of an IC card with which all the key information corresponding to each segment carries out reading appearance only of the time of the right, and a result is confirmed is proposed.

[0003]

[Problem(s) to be Solved by the Invention] Although it enciphered and the secrecy of an in-house data is protected by the above-mentioned conventional data unjust reading defense method in memory in case data are read in an IC card, the secrecy of the data in memory can be unfairly read by secret data being held, destroying or disassembling an IC card into the memory in an IC card, sucking up an in-house data compulsorily by a ROM writer etc., analyzing an in-house data, and decoding codes, such as a key value.

[0004]

[Means for Solving the Problem] In order to access the memory data in a direct IC card by a ROM writer etc. according to this invention When the body of an IC card is destroyed or disassembled, the bus which connects memory with the cell which suited the open-circuit condition contacts and a bus connects by the switch equivalent function interlocked with opening of the body of an IC card Or when the light from the outside hits and the resistivity of the optical device connected to the bus which connects memory with a cell becomes high The secrecy of the data in memory can be protected by eliminating all or some of data which an electrical potential difference joins the external terminal for data elimination of memory, and is held within memory.

[0005]

[Embodiment of the Invention] Hereafter, the desirable example of this invention is explained.

[0006] Drawing 1 expresses the part about invention of claim 1 among the circuit diagrams of an IC card. If a switch 20 is pushed, a contact 21 and a contact 22 will be connected through a switch 20, and memory 10 will be connected with a cell 30.

[0007] Drawing 2 shows the condition of the switch section in case the body of an IC card is sealed.

[0008] When the body of an IC card is sealed, a switch 20 cannot touch a contact 21 and a contact 22 because of the stopper 50 connected to the body 1. for this reason, memory 10 is connected with a cell 30 -- not having -- data elimination -- business -- in order for an electrical potential difference not to join

---

the external terminal 11, the data in memory are held.

[0009] Drawing 3 shows the condition of the switch section at the time of destroying or disassembling an IC card.

[0010] When an IC card is destroyed or disassembled, for the repulsive force of a spring 60, a stopper 50 is pushed, a contact 21 and a contact 22 are connected through a switch 20, and memory 10 is connected with a cell 30. For this reason, the electrical potential difference from a cell 30 joins the external terminal 11 for data elimination, and the data in memory are eliminated.

[0011] Drawing 4 expresses the part about invention of claim 2 among the circuit diagrams of an IC card. Memory 10 is connected with the cell 30 at the optical device 70 and juxtaposition to which resistivity becomes high in proportion to the quantity of light.

---

[0012] Since an external light does not shine upon the optical device 70 when the body 1 of an IC card is sealed, the resistance of the optical device 70 is low. data elimination of memory 10 by which parallel connection is carried out to the optical device 70 for this reason -- business -- in order only for an electrical potential difference smaller than the threshold for eliminating the data in memory to join the external terminal 11, the data in memory are held.

[0013] When an IC card is destroyed or disassembled, as for the resistance of the optical device 70, an external light becomes large in the optical device 70. this sake -- data elimination of memory 10 -- business -- a bigger electrical potential difference than the threshold for eliminating the data in memory joins the external terminal 11, and the data in memory are eliminated.

[0014] As mentioned above, in invention in claim 1 and claim 2, when a third party is going to read the data in memory of an IC card unfairly and an IC card is destroyed or disassembled, the secrecy of the data in memory can be protected by eliminating the data in memory.

[0015]

[Effect of the Invention] When the body of an IC card is destroyed or disassembled according to this invention, the bus which connects memory with the cell which suited the open-circuit condition contacts and a bus connects with the body of an IC card Or when the light from the outside hits and the resistivity of the device connected to the bus which connects memory with a cell becomes high All or some of data which an electrical potential difference joins the external terminal for data elimination of memory, and is held within memory can be eliminated, and the secrecy of the data in memory can be protected.

---

[Translation done.]